

appreciates AirTouch's concern that the paperwork burden on carriers should be minimized as much as possible. Law Enforcement is well aware of the possible paperwork burden placed upon carriers by the Commission's proposed rules, and thus has sought to minimize them to the extent possible. Law Enforcement, however, believes that evidentiary requirements far outweigh the burdens here. In order to effectuate a valid electronic surveillance, Law Enforcement must ensure that the intercept meets the evidentiary threshold needed to introduce the electronic surveillance evidence into a court of law. Thus, the proposal that certification be prepared only by the employee or officer responsible for overseeing the interception activity is both reasonable and appropriate.

76. The certification should also set forth the identities and functions of all carrier personnel who have knowledge of, or access to, information or facilities associated with the intercept. If, as Law Enforcement has suggested in its response to Paragraph 30 of the NPRM, each of those employees or officers is a designated person, the individual personnel records of those individuals should contain the requisite certification concerning non-disclosure of intercept information. Moreover, Law Enforcement proposes that any such document include an additional item stating that the signatory understands that unauthorized disclosure of intercept information is an actionable offense, potentially subjecting its perpetrator to criminal or civil penalties, including imprisonment or fine, or both.

77. Law Enforcement, however, still differs with the Commission's proposed Item 4. Law Enforcement continues to believe that Item 4 should be deleted because it is impossible for carrier security personnel to know, in real time, when the interception must lawfully terminate. Moreover, with respect to the first item on the list, the "telephone number(s) or the circuit identification number(s)," Law Enforcement believes that this category should be modified slightly to include the telephone number(s) *and* the circuit identification number(s). This is the phrasing used by the Commission in connection with

the record keeping requirement addressed in Paragraph 32 of the NPRM. In addition, Law Enforcement strongly urges the Commission to broaden the category to include the subscriber identifier(s) (IMSI or MIN number(s)) and the terminal identifier(s) (IMEI or ESN number(s)) that would apply to interceptions of wireless communications. These identifiers should be included because, in wireless networks, routing numbers and line identities may be insufficient to connect a particular telephone number to a specific subscriber.⁷⁶

78. Finally, Law Enforcement wishes to reiterate that the paperwork burden should never impede the timeliness with which intercept requests are implemented. The timeliness with which Law Enforcement receives such information is critical to the maintenance of the integrity and evidentiary validity of electronic surveillance information.

5. Reports of Violations-Compromises

79. Law Enforcement, SBC, GTE, Ameritech, BellSouth, and Bell Atlantic Mobile all concur that it is a carrier's affirmative obligation to report violations of its security policies and procedures and compromises, or suspected compromises, of authorized electronic surveillance to the affected law enforcement agency, or agencies, when the compromise is related to the potential unauthorized disclosure of a surveillance or other law enforcement activity. Law Enforcement considers this to be essential because of the potential threat to the safety of witnesses, undercover agents, and intercept subjects that a compromise could represent. Carrier technical personnel should be required to report such

⁷⁶ IMSI numbers are "International Mobile Subscriber Identities;" MIN numbers are "Mobile Identity Numbers;" IMEI numbers are "International Mobile Equipment Identities;" and ESN numbers are "Electronic Serial Numbers." See Cellular Radio Telecommunications Intersystem Operations Signaling Protocols (Interim Standard), TIA/EIA/IS-41.5-C (February 1996).

compromises, or suspected compromises, to the carrier security office immediately upon discovery. At a minimum, Law Enforcement strongly urges that the Commission require that no more than two (2) hours be allowed to elapse between the time of the discovery that an intercept has been compromised, or is suspected of being compromised, and the report of that fact to the affected law enforcement agency or agencies.

80. Law Enforcement also advocates that in the event a carrier acquires information that leads it to suspect that its employee may have engaged in illegal surveillance activity on his own, that information should be reported immediately to the FBI or the cognizant law enforcement agency for further investigation.⁷⁷ At a minimum, Law Enforcement presumes that the employee would be reassigned immediately pending the outcome of the investigation. Law Enforcement, based upon past experience, understands this to be the practice now followed by most carriers.

81. Law Enforcement believes that the standard that should be applied in determining whether an intercept may have been compromised is the standard of reasonable suspicion. In this regard, carrier personnel should be required to report objective facts that would reasonably give rise to the suspicion that an intercept has been compromised. Upon discovery of such facts, carrier personnel should be required to report the suspected compromise to the security office, which, in turn, would report it to the law enforcement agency involved.

⁷⁷ To allay the concerns of NTCA, Law Enforcement is only proposing, in this context, that carriers report illegal electronic surveillance. Specifically, under 18 U.S.C. § 2511, illegal electronic surveillance requires intentional, as opposed to negligent or inadvertent, conduct. *See also* 18 U.S.C. § 2520 (providing a good faith defense).

82. Law Enforcement, however, believes that such violations and compromises of intercepts should be reported to the Commission every two years when a carrier must recertify that it is complying with the security policies and procedures mandated by CALEA and its implementing regulation.⁷⁸ In addition, Law Enforcement and SBC agree that reports made to the Commission relating to compromises should be strictly confidential, and not put in the public record. Law Enforcement believes that such reports would enable the Commission to exercise more effectively its continuing jurisdiction over CALEA-related matters.

6. Timeliness

83. Law Enforcement continues to believe that one of the most critical factors affecting the efficacy of electronic surveillance is the timeliness with which intercepts are implemented. Section 103 of CALEA requires carriers to be capable of "*expeditiously* isolating, and enabling the government to intercept, all wire and electronic communications within that carrier's network . . ." and "*rapidly* isolating, and enabling the government to access, call identifying information that is reasonably available to the carrier." 47 U.S.C. § 1002. Thus, Law Enforcement disagrees with SBC's comments that the Commission should refrain from adding administrative rules relating to timeliness of effectuating a court ordered electronic surveillance.

84. Law Enforcement is well aware that the more cumbersome a carrier's implementation procedure, the greater the likelihood that investigations will be hampered by unnecessary delays. Therefore, to facilitate the CALEA requirement that carriers respond promptly to interception orders and provide information "*expeditiously*" and "*rapidly*," the

⁷⁸ See *infra* "Certification of CALEA Requirements."

Commission should require that carriers receiving interception orders or certifications complete their internal approval and documentation process and implement the interception within eight (8) hours of receiving the court order, certification, or consent. For exigent circumstances, in cases under 18 U.S.C. §§ 2518(7), 3125, no more than two (2) hours should be allowed to elapse before an interception, pen register, or trap and trace is implemented. These time periods warrant the further requirement that carriers have a designated security officer and designated technical personnel available, either on duty or on call by pager, 24 hours a day, seven (7) days a week.

85. Law Enforcement still believes that the accelerated 2-hour time period that should apply to the duty of carriers to report compromises of intercepts to Law Enforcement should also apply to reporting intercept malfunctions following their discovery. As discussed above, the compromise of an intercept poses an immediate danger to the safety of any undercover personnel who may be involved in the investigation and perhaps to the subjects of the intercept as well. So too, malfunctioning intercepts not only result in the loss of critical evidence, but they also endanger public safety by inhibiting Law Enforcement's ability to respond in emergency circumstances. Moreover, a time period longer than two (2) hours would result in a needless waste of the law enforcement resources being dedicated to an inoperative electronic surveillance.

86. In Paragraph 33 of the NPRM, the Commission asks for comment on additional information that carriers should be required to provide to Law Enforcement. Law Enforcement reiterates that carriers should be required to maintain and have accessible to Law Enforcement a point or points of contact available twenty-four (24) hours a day, seven (7) days a week to ensure Law Enforcement access to the installation, monitoring, and maintenance of pen register, trap and trace, communication content, and other related electronic surveillance functions. Such a point of contact is commonly in place today with

regard to carriers and law enforcement officers specializing in electronic surveillance. Law Enforcement supports the efforts by the carriers and Commission to meet this obligation in the least burdensome manner possible.

7. Certification of CALEA Requirements

87. Law Enforcement still contends that both Title III and CALEA apply across the board to small and large carriers alike. Law Enforcement also believes that public safety and security concerns should not vary according to the geography or the size of the carrier. Therefore, the CALEA regulatory requirements developed by the Commission should be made to apply equally to all CALEA-covered entities, and a multi-tiered regulatory scheme, whether based on carrier revenues or number of subscribers, should be rejected by the Commission.

88. For these reasons, Law Enforcement continues to disagree with the Commission's proposal, stated in Paragraph 35 of the NPRM, which defines a category of "small telecommunications carriers" based on \$100 million annual operating revenues. Likewise, Law Enforcement has several concerns about the Commission's proposal, in Paragraph 35, to permit "small carriers" to elect to file a certification that its procedures are consistent with Commission rules regarding CALEA. Such a proposal likely would quickly become unworkable and, indeed, could lead to the imposition of an even greater administrative burden on carriers and the Commission. Furthermore, the \$100 million cutoff would effectively eliminate all but about 21 of the thousands of telecommunications carriers covered by CALEA from the more stringent regulatory requirements.⁷⁹

⁷⁹ In 1994, approximately 21 local exchange carriers had revenues above \$100 million. *See* 1995 America's Network Directory (*citing* USTA 1994 Holding Company Report).

89. A majority of commenters contend that all competitive carriers, not just small carriers with revenues less than \$100 million, should have the opportunity to take advantage of the self-certification procedures that the Commission has proposed.⁸⁰ The commenters premise their arguments on the belief that streamlined procedures would promote the public interest, thereby reducing the administrative burden and expense and thus increasing efficiency. In addition, AirTouch asserts that it is not clear how competition would be enhanced if market participants were required to divulge their internal policies and practices.⁸¹ Based upon the carriers' submissions, Law Enforcement now agrees that all carriers, regardless of their size, need only certify initially that they are in compliance with the security policies and procedures mandated by CALEA and its implementing regulation, and then re-certify to such compliance every two (2) years thereafter. Requiring only such certification will substantially decrease the proposed reporting burdens placed on carriers. Moreover, Law Enforcement agrees with PageNet that carriers should only provide their internal security compliance manuals upon request by the Commission or Law Enforcement.

90. In order to ensure standard security policy procedures, Law Enforcement advocates that the Commission develop standardized forms to assist carriers in designing CALEA compliance manuals.⁸² This would ensure that identical standards would be applicable to large and small carriers alike. The Commission could even issue a manual

⁸⁰ *Accord* PageNet, 360 Degree Communications, PrimeCo Personal Communications, and PCIA, CTIA, and AirTouch.

⁸¹ AirTouch further states that given the fact that carriers have a long history of meeting Law Enforcement's interception requirements without invading customers' substantial privacy interests, there is no reason to now require competitive carriers to submit their internal compliance manuals to the Commission for review.

⁸² *Accord* PowerTel.

containing a template set of security policies and procedures, which the adoption of and adherence to could be deemed by the Commission to be CALEA compliant.

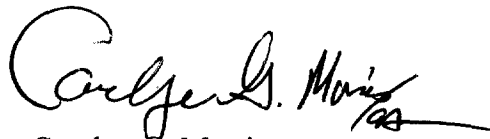
91. Law Enforcement is willing to work with Commission staff to develop the appropriate forms, but wishes to emphasize that their primary concerns are that the timeliness, accuracy, security, and evidentiary validity of surveillance information be protected. Beyond that, it may be more appropriate for the Commission, together with interested trade associations and individual carriers, to lead such an effort.

VII. CONCLUSION

92. Law Enforcement commends the efforts of all commenters to this NPRM and respectfully requests that the Commission consider carefully our positions herein submitted on many of the comments made by others. We also respectfully request that the Commission adopt the additional measures proposed in our original comments to the NPRM.

Respectfully submitted,

FEDERAL BUREAU OF INVESTIGATION

A handwritten signature in cursive script, reading "Carolyn G. Morris".

Carolyn G. Morris

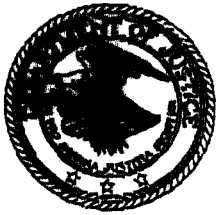
Assistant Director

Information Resources Division

14800 Conference Center Drive Suite 300

Chantilly, Virginia 20151

APPENDIX A



Office of the Attorney General
Washington, D. C. 20530

JAN 22 1998

Mr. Matthew J. Flanigan
President
Telecommunications Industry Association
2500 Wilson Boulevard
Suite 300
Arlington, VA 22201-3834

Dear Mr. Flanigan:

This letter responds to concerns expressed recently by members of the telecommunications industry with respect to the taking (or forbearance) of enforcement actions under the Communications Assistance for Law Enforcement Act (CALEA).

As you know, in enacting CALEA, Congress intended to preserve law enforcement's electronic surveillance capabilities and to prevent those capabilities from being eroded by technological impediments related to advanced telecommunications technologies, services, and features. To that end, Congress also specified that the solutions to overcome these impediments must be implemented within four years of the date of CALEA's enactment. The deadline for carriers to comply with section 103 of CALEA is October 25, 1998.

The Federal Bureau of Investigation (FBI) is working diligently with members of the industry, both individually and collectively, to ensure that the carriers and manufacturers are able to meet the deadline. In those situations where the carrier can foresee that it will not be able to meet the deadline because the manufacturer has yet to develop the solutions, the FBI is prepared to enter into an agreement with the manufacturer of the carrier's equipment wherein both parties (the FBI and a manufacturer) would agree upon the technological requirements and functionality for a specific switch platform (or other non-switch solution) and a reasonable and fair deployment schedule which would include verifiable milestones. In return, the Department will not pursue an enforcement action against the manufacturer or carrier as long as the terms of the agreement are met in the time frames specified. The Department will not pursue enforcement action against any carrier utilizing the switch platform (or non-switch solution) named in the agreement. Finally, the Department will support a carrier's petition to the Federal Communications

Mr. Matthew J. Flanigan
Page 2

Commission (FCC) for an extension of the compliance date for the equipment named in the agreement and for the length of time specified in the agreement. Where an agreement has been signed, if a dispute arises between the manufacturer and the FBI which cannot be resolved, the manufacturer may appeal the issue directly to the Attorney General or her designate for prompt resolution.

Your continued willingness to work toward solutions which will support law enforcement's electronic surveillance requirements is greatly appreciated.

Sincerely,

A handwritten signature in cursive script, appearing to read "Janet Reno", is written over the typed name.

Janet Reno

APPENDIX B

**COMMUNICATIONS ASSISTANCE FOR
LAW ENFORCEMENT ACT
(CALEA)**

IMPLEMENTATION REPORT

January 26, 1998

**Prepared by:
Department of Justice
Federal Bureau of Investigation
Information Resources Division
14800 Conference Center Drive, Suite 300
Chantilly, Virginia 20151**

TABLE OF CONTENTS

	Page
<i>i.</i> Non-Disclosure Agreements	1
I. Executive Summary	2
II. Introduction	5
III. Activities	6
IV. Results	8
V. Conclusion	15
Appendices	
A. Chronology of meetings with industry	16
B. Solution availability timeline	18
C. Punch list capabilities description	19

NON-DISCLOSURE AGREEMENTS

In the process of gathering data for this report, the Federal Bureau of Investigation (FBI) was provided access to significant amounts of information considered proprietary by solution providers¹ and carriers. This information was, and is, vital to the FBI's ongoing efforts to work cooperatively with the telecommunications industry on the development of a CALEA solution. The FBI is very sensitive to concerns expressed by industry regarding release of this data to outside parties, and has signed non-disclosure agreements that limit the release of any proprietary information.

Citing those non-disclosure agreements, some solution providers have required that certain proprietary information provided to the FBI during this initiative be withheld from this report. However, solution providers have expressed a willingness to privately brief interested Members of Congress on specific technical and price feasibility as well as development schedules.

¹ The term "solution providers" refers to traditional telecommunications equipment manufacturers as well as other companies that are pursuing a CALEA solution.

I. EXECUTIVE SUMMARY

The Conference Committee Report (H. Rpt. 105-405) accompanying the 1998 Justice Appropriations Act (P.L. 105-119) directs the Department of Justice (DOJ) to submit to the Committees on Appropriations a report that includes (1) cost estimates for development and deployment of the proposed CALEA solution; (2) a timeline for development and deployment of the solution; and (3) two signed cooperative agreements with appropriate telecommunications carriers and/or equipment manufacturers. These requirements were the result of a meeting called by Chairman Harold Rogers, House Appropriations Subcommittee for the Departments of Commerce, Justice, and State, on October 22, 1997, and attended by representatives of the DOJ, FBI, and the telecommunications industry to discuss the status of CALEA implementation.

This report describes the substantial progress made to date in response to the Conference Committee Report. In so doing, the report provides a snapshot of ongoing FBI and industry CALEA implementation efforts. Information exchanged as a result of this initiative has greatly assisted all parties as they continue to work toward development and deployment of CALEA solutions. At the conclusion of an October 22, 1997 meeting with representatives of law enforcement and the telecommunications industry, DOJ set out to achieve the following goals by January 4, 1998:

1. Assess the technical feasibility of certain CALEA capability requirements (punch list), and determine the price of those capabilities
2. Obtain two signed "cooperative agreements"
3. Obtain a timeline for possible CALEA solution deployment.

Status

In response, the FBI assigned teams of personnel, including representatives of state and local law enforcement, to specific solution providers to expand ongoing technical and price discussions and enter into cooperative agreements if appropriate. Teams were assigned to Nortel, Lucent Technologies (Lucent), Siemens Telecom Networks (Siemens), and Motorola Cellular Infrastructure Group (CIG) due to the significance of their switching platforms to law enforcement. Additionally, the FBI pursued discussions with Bell Emergis, a company developing a network-based CALEA solution. Several telecommunications carriers were also approached to aid law enforcement in interpreting solution information and providing network impact assessments. Continuing on efforts begun in July 1997, the FBI held over 20 substantive technical and business meetings with members of industry between November 4, 1997 and December 15, 1997 (see Appendix A). CALEA implementation has reached a point where:

- Certain solution providers are expected to make available specific switch-based

- and network-based CALEA solutions in 1998;²
- One major carrier anticipates testing a network-based CALEA solution in early 1998;
- Solution providers participating in this initiative have the technical ability to meet the intent³ of nearly all CALEA capability requirements;
- Agreements for continued cooperation between industry and law enforcement are in place. Additional agreements are expected in the coming weeks.

As a result of these efforts, a clearer picture of CALEA's technical feasibility, potential solution prices and deployment timelines has emerged. Law enforcement and solution providers now have a shared understanding of the technical feasibility of a switch-based CALEA capability, yielding significant benefits to all parties. For example, Nortel stated that this understanding may result in a 25 percent reduction in the level of the development effort that was previously estimated. This solution includes the punch list capabilities. These discussions have also allowed switch manufacturers to provide law enforcement with more detailed estimates of solution prices and deployment timelines.

Additionally, the FBI continues to have very promising discussions with Bell Emergis, a company pursuing a network-based CALEA solution. Bell Emergis claims to have completed development of a CALEA solution that meets most of CALEA's capability requirements. Bell Emergis has proactively sought to establish contact with the carrier community, and the initial response from various carriers has been encouraging. The company intends to have its solution available to carriers in the second quarter of 1998, before the October 25, 1998 capability compliance date. The FBI is currently analyzing the product's technical and fiscal feasibility.

The following table summarizes the information provided by industry during the preceding two months. In addition to the solution provider data presented below, GTE, a carrier, has forwarded a signed cooperative agreement detailing the conditions under which it will continue to provide assistance to the FBI. The FBI expects to use this proposal as the basis for further negotiation with GTE.

² A more complete description of the differences between switch-based and network-based CALEA solutions is provided in section III.

³ Solution providers have either confirmed the ability to meet the CALEA capability requirements or supply the equivalent information by alternative means.

Solution Provider	Technical Feasibility	Price Estimate	Solution Availability	Agreement Status
Motorola EMX-2500, 5000	Partial	*	*	Draft AIP [†] received by the FBI
Lucent 5ESS	Yes ^{††}	*	3Q1999	None
Siemens EWSD	Partial	*	Two phases 1Q2000 -1Q2001	None
Nortel DMS-100	Partial	*	Two phases 4Q1998 - 2Q2000	Pending
Bell Emergis	Partial	Estimate supplied (see page 13)	3Q1998	Signed MOU ^{†††} received by the FBI

* Information made available to the FBI, but covered under existing non-disclosure agreements with industry. Data has been withheld from this report at the manufacturer's request.

† Agreement in Principle (AIP): Written agreement between parties to continue working toward development of a solution.

†† At the request of the manufacturer, no face-to-face meetings have been held to date between Lucent and the FBI to confirm technical feasibility.

††† Memorandum of Understanding (MOU): Written agreement between parties to continue working toward development of a solution.

A distinction can be drawn between solution providers' partial ability to meet CALEA's capability requirements and its ability to meet the intent of those same requirements. In some cases, individual switch designs and architectures constrain solution providers' ability to fully meet CALEA's capability requirements. According to solution providers, the technical obstacles for some switches are so severe that the provision of certain CALEA capability requirements is either technically infeasible or cost prohibitive. In these cases, the FBI has noted the solution provider as having a "partial" ability to meet CALEA's capability requirements. In other cases, technical limitations have led to discussions of alternative means of providing necessary evidentiary and minimization data to law enforcement. Where alternative methods have been identified by a solution provider, the FBI has noted that the solution provider has the ability to meet the "intent" of CALEA's capability requirements.

Price and technical information has afforded the FBI greater insight into when and how much money may be required from the Telecommunications Carrier Compliance Fund (TCCF). It is anticipated that this information flow will continue as solution providers proceed through their normal business processes, allowing the FBI to more accurately estimate fiscal year reimbursement needs. In fact, Nortel has told law enforcement that the first phase of their switch-based CALEA solution may be available for purchase by carriers as early as the third quarter of 1998.

Additionally, Bell Emergis has indications that several carriers are very interested in its network-based solution. The FBI has been approached by one carrier to participate in testing the Bell Emergis solution in early 1998. At the request of the carrier, its name is being withheld from this report. Should these solutions prove to be CALEA-compliant and reasonable in cost, the FBI could begin the reimbursement process during Fiscal Year (FY) 1998.

II. INTRODUCTION

As the end-user of the CALEA solution, law enforcement has a great deal at stake in ensuring the necessary functionality of any developed solution. The evidentiary information obtained through electronic surveillance is critical to preserving the safety and security of the American public through the apprehension and successful prosecution of criminals. A solution that does not meet CALEA capability requirements puts at risk evidentiary information required by law enforcement and prosecutors to obtain a conviction in a court of law.

Despite law enforcement's dependence on the functionality of a solution, section 103 of CALEA prohibits law enforcement from requiring specific solution requirements. Additionally, unlike traditional government procurement efforts, law enforcement is unable to influence a specific solution price. Rather, CALEA is a reimbursement effort, with law enforcement as the entity for evaluating proposed solutions, determining the reasonableness of any price and reimbursing industry for certain eligible CALEA costs. Law enforcement's role throughout the design, development and deployment of a CALEA solution is twofold: first, to assist industry in its understanding of law enforcement's electronic surveillance capability requirements; and second, to evaluate any solution's technical feasibility and cost effectiveness.

In an attempt to move the CALEA implementation process forward, Chairman Rogers met with representatives of the telecommunications industry and law enforcement on October 22, 1997 to discuss several outstanding issues regarding CALEA's implementation. At the conclusion of the meeting, Chairman Rogers requested that DOJ and industry work together to provide the Appropriations Committee with CALEA solution cost and schedule information by January 4, 1998.⁴ The Conference Committee Report (H. Rpt. 105-405) accompanying the 1998 Justice Appropriations Act formalized these requirements into a request for a report. In accordance with the Conference Committee Report, the FBI worked with solution providers and carriers in a cooperative effort to achieve the following specific goals, summarized below:

Prepare per-platform technical feasibility studies for CALEA capabilities, including punch list items, to aid in determining price

The FBI worked with solution providers to obtain a shared understanding of the technical feasibility of CALEA capability requirements. Once complexity and technical feasibility were better understood, a level of effort comparison to features of similar complexity was employed to estimate a CALEA solution price.

Execute two cooperative agreements with industry

The FBI sought to use the cooperative agreement initiative to accomplish two objectives: first, to create a mutually acceptable process by which solution providers and carriers could share solution price, technical and development information with law enforcement;

⁴ Pursuant to a letter dated December 31, 1997 from Assistant Attorney General for Administration Stephen R. Colgate to Chairman Harold Rogers, the Committee was advised this report would be delayed until January 26, 1998.

and second, to lay the foundation for follow-on contractual agreements for the reimbursement of carriers for the purchase of commercially available solutions.

Obtain an accurate timeline for solution deployment

Solution providers will develop and release CALEA solutions in accordance with their established business processes and cycles. The FBI has no influence over these solution provider determined development cycles. Upon obtaining a technical feasibility assessment, the FBI asked solution providers to provide product release schedules for the CALEA feature.

It is important to note that telecommunications switch manufacturers will develop the CALEA feature as they would any other feature to be included in a software release. That development process can be described as: identification of customer needs, feature functionality specification, feature development with carrier participation, testing in both a laboratory environment and as a first office application in carriers' network, and systems deployment. It is clear that some manufacturers are further along in the development process than others. Indeed, some manufacturers are well into the CALEA solution development stage, while some are still working with law enforcement to refine feature requirements. In the normal course of the development process, it is expected that more detailed technical and price information will be made available to law enforcement to make an assessment of the solution. The FBI will continue working with each individual manufacturer in an appropriate manner to move their processes forward as quickly as possible.

III. ACTIVITIES

The FBI relied on previously established working relationships with key members of the telecommunications industry to develop the information in this report. Consistent with the CALEA Implementation Plan submitted to Congress in March 1997, the FBI had established relationships with solution providers of certain prioritized switch equipment. Previous analyses of historical intercept activity demonstrated that approximately 90 percent of wireline interceptions occurred on Nortel, Lucent, and Siemens switches.⁵ Motorola was identified due to its significant presence in the wireless market and its willingness to participate.

Competitive sensitivities, market positions, switch architectures and product development cycles vary widely among switch manufacturers. To maximize its efforts, the FBI developed a customized outreach approach for each solution provider. Five "Industry Teams" were formed, with each team assigned a specific solution provider with whom to continue technical and price discussions and sign cooperative agreements, if appropriate. Teams were assigned to Nortel, Lucent Technologies, Siemens, and Motorola due to the significance of their switching platforms

⁵ Based on a 1996 nationwide FBI survey of law enforcement and industry electronic intercept records between January 1993 and March 1995.

to law enforcement. Additionally, discussions were also pursued with Bell Emergis, a firm developing a network-based CALEA solution.

A switch-based CALEA solution requires modifying internal switch software, and potentially necessitates hardware changes. A network-based solution does not require that a switch manufacturer make internal switch software or hardware modifications in order for the end-office switch utilized by a carrier to provide the capability requirements of CALEA. Instead, carriers choosing to employ a network-based solution must make only minor configuration changes to individual switches. These limited changes are expected to be easy for a carrier to implement and are consistent with normal carrier modifications, such as changes to switch translations (the instruction set necessary for call direction and completion). No development work on the part of a switch manufacturer would be necessary for the switch itself when network-based solutions are used.

As any CALEA solution will be deployed on networks owned and operated by telecommunications carriers, carrier perspective and input into the design, development and deployment activities is vital. Several carriers were approached to aid law enforcement in obtaining and interpreting technical and price information provided by solution providers. Additionally, the FBI sought carrier cooperation in providing, when appropriate, network impact assessments and access to lab facilities for solution testing.

Each industry team, as mentioned previously in this section, was led by an FBI Program Manager and included a representative from state and/or local law enforcement. The teams were supported by subject matter experts familiar with the technical operations of the solution providers' product line.

Technical and Price Feasibility Initiative

Once formed, industry teams contacted their respective solution provider to initiate a series of detailed technical meetings to discuss CALEA solution feasibility. During these substantive meetings, law enforcement's requirements were translated into specific switch functionalities to determine how (and whether) a capability was feasible on a given switch platform. The goal of the effort was to clarify CALEA capability requirements within the context of (and with regard to any technical constraints inherent in) each manufacturer's switch or proposed CALEA solution.

Whenever possible, where a capability presented serious technical obstacles for a particular solution, technical alternatives that provided law enforcement with the necessary evidentiary and minimization data sought by that capability were identified and evaluated. However, detailed technical alternatives for CALEA capabilities are not presented in this report due to non-disclosure agreements. After discussing CALEA's requirements for reasonableness in cost reimbursements with manufacturers, the FBI relied solely on industry-provided price estimates.

Cooperative Agreement Initiative

Concurrently with the technical feasibility initiative, the FBI approached manufacturers and carriers in order to clarify the roles and responsibilities of all parties through cooperative agreements. The FBI's main objective in signing cooperative agreements was twofold. First, the FBI sought to create a mutually acceptable process whereby industry and law enforcement could continue to share relevant cost, schedule, and technical data. Second, the agreements were intended to lay the foundation for follow-on contractual agreements for the reimbursement of carriers for the purchase of commercially available solutions.

The appropriate form and content of the cooperative agreement document had to be determined. The document needed to address the competitive sensitivities of industry, while still providing a meaningful document that committed the parties to move the process forward. To accomplish these objectives, Agreements in Principle (AIP) or Memoranda of Understanding (MOU) for solution providers and a Statement of Work (SOW) for carriers were drafted. The AIPs or MOUs committed solution providers to supply the Government with technical and price information and dates for solution availability, while the SOWs sought the carriers' perspective in interpreting technical and price data provided by solution providers. These documents were modified as necessary in response to the specific comments of each solution provider or carrier.

Solution Deployment Timeline Initiative

Solution providers were able to provide law enforcement with technical feasibility and approximate dates for solution availability. These availability dates vary depending on how far a solution provider has progressed in its solution-development cycle (see Appendix B). Since carriers cannot begin their deployment process until a solution is available, these individual variations will influence the timeline for CALEA deployment. In several cases, manufacturers plan to release their CALEA solutions over multiple software product releases.

IV. RESULTS

Varying levels of industry cooperation and the presence of non-disclosure agreements have impacted the level of detail and quantity of information provided in this report. Some solution providers were very receptive to the FBI's data requests, sharing detailed, per-capability technical and price data with law enforcement. Other solution providers were more reluctant to participate, providing only aggregate CALEA price and technical data. Still others provided the FBI with information, but did not allow its publication in this report.

Additionally, technical feasibility, price, and deployment timeline information presented in this report is based solely on information provided by industry. By necessity, the FBI has relied on industry to faithfully and accurately reflect CALEA's complexity and price based on solution providers' inherent knowledge of their switching platform and their carriers' network architecture.

As more carriers and solution providers become involved in the weeks and months ahead, the FBI anticipates additional data will be forthcoming from industry. As it has done in the past, when the information is made available to the FBI, appropriate analyses will be performed.

Technical Feasibility Initiative

The technical feasibility of CALEA required assistance capabilities as outlined in section 103 varies among switching platforms due to differences in individual switch architectures and solution approaches. (For a description of the capabilities missing from the current standard, i.e., punch list capabilities, see Appendix C.) Solution providers are able to characterize the relative complexity of the development of punch list items for their switching platforms. A capability characterized as easy by one solution provider may be characterized as very difficult (i.e., though not technically impossible) by another. Where technical constraints existed, face-to-face discussions between law enforcement and solution providers often resulted in the identification of technical alternatives that provided law enforcement with the necessary evidentiary and minimization assistance sought by that particular capability. As a result, technical concerns regarding CALEA's capability requirements previously considered technically difficult to develop have diminished.

It is important to note that the level of technical complexity is subject to the interpretation of each solution provider and cannot be compared with other solution providers' analyses. The following paragraphs describe solution providers' technical feasibility information permitted to be disclosed under non-disclosure agreements.

Motorola (EMX 2500, EMX 5000)

The FBI held four technical discussions with Motorola to determine technical feasibility on the EMX 2500 and 5000 cellular switching platforms. During the course of those meetings, Motorola provided the FBI with detailed technical feasibility information for its proposed CALEA solution.

Motorola assessed the punch list capability items as technically feasible with the following exceptions which they characterize as more technically difficult:

- Capability #3 - Access to subject-initiated feature key dialing and signaling
- Capability #4 - Notification Message, In-band and Out-of-band signaling
- Capability #9 - Feature Status Message
- Capability #11 - Separated Delivery.

Based on non-disclosure agreements, Motorola requested that more detailed technical feasibility information be withheld from this report. Motorola and the FBI have agreed to continue evaluating alternative methods of meeting CALEA's capability requirements.

Nortel (DMS-100 Family)

The FBI and Nortel held five technical meetings and frequent telephone calls to discuss the technical feasibility on its DMS-100 family of switches. The DMS-100 family of switches is technically capable of meeting the intent of all of law enforcement's CALEA requirements. In keeping with normal product-development processes, Nortel's CALEA solution is scheduled to be implemented in a phased approach of at least two software releases.

Nortel assessed the development effort necessary for the punch list capability items as low to moderate with the following exceptions:

- Capability #2 - Party Hold, Party Join, Party Drop Message, as described by law enforcement, is viewed by Nortel as difficult. However, Nortel can generally meet the intent of this requirement by alternative means.
- Capability #3 - Access to subject-initiated feature key dialing and signaling
- Capability #4 - Notification Message, In-band and Out-of-band signaling
- Capability #9 - Feature Status Message.

These requirements (#3, #4, and #9), as described by law enforcement, are viewed by Nortel as very difficult. However, Nortel can meet the intent of these requirements by alternative means.

- Capability #11 - Separated Delivery - This requirement, as described by law enforcement, is viewed by Nortel as extremely difficult. However, Nortel has described an alternative that law enforcement is currently evaluating.

Lucent (5ESS)

While technical feasibility information for the 5ESS was provided to the FBI, at Lucent's request, no face-to-face meetings have been held to date with the FBI as part of this initiative. Lucent's current assessment is that all CALEA capabilities are technically feasible on the 5ESS. Face-to-face technical meetings are expected between Lucent and the FBI beginning in early 1998, at which time the FBI will be better able to evaluate Lucent's current estimate of technical feasibility.

Lucent assessed the development effort necessary for the punch list capability items as low to moderate with the following exceptions:

- Capability #11 - Separated Delivery - This requirement, as described by law enforcement, is viewed by Lucent as extremely difficult.

Siemens (EWSD)

The FBI and Siemens held six technical meetings to discuss technical feasibility on the EWSD switching platform. The EWSD switch platform is technically capable of meeting the intent of all of law enforcement's CALEA requirements. Siemens does have concerns based on the technical complexity of certain capability requirements and available staff resources. These concerns have resulted in Siemens' decision to implement CALEA in a phased approach incorporating two or more software releases.

Siemens assessed the development effort necessary for the punch list capability items as low to moderate with the following exceptions:

- Capability #1 - Content of conference calls
- Capability #10 - Dialed digit extraction, as described by law enforcement, is viewed by Siemens as extremely difficult.

Siemens' rough estimate of availability of these two punch list capabilities is 2001. Based on this information, and until such time that these capabilities are developed, the FBI has noted Siemens' ability to meet CALEA's capability requirements as "partial."

Bell Emergis

Bell Emergis' network-based solution does not require the modification of each and every end-office switch. Instead, the Bell Emergis solution would operate in conjunction with the Signaling System 7 (SS7) network, which today provides inter-switch call set-up for approximately 90 percent of the access lines nationwide. Both wireline and wireless networks utilize the SS7 network in providing telecommunications service.

Since July, 1997 the FBI and Bell Emergis held numerous detailed technical meetings to assess the Bell Emergis solution's ability to meet CALEA requirements. Bell Emergis claims its solution is technically capable of meeting virtually all of CALEA's capability requirements. Bell Emergis is proactively pursuing a partnered approach with the carrier community, which it anticipates will enhance its ability to meet CALEA capability requirements. The initial response from several carriers has been encouraging. The Bell Emergis solution is expected to undergo carrier evaluation during the first quarter of 1998. Carriers have expressed an interest in involving the FBI in this process.

Bell Emergis assessed the development effort necessary for the punch list capability items as low to moderate with the following exceptions:

- Capability #3 - Access to subject-initiated feature key dialing and signaling
- Capability #4 - Notification Message, In-band and Out-of-band signaling